Construction géométrique de (3,3)-isogénies depuis un produit de courbes elliptiques

Rémy Oudompheng

11 octobre 2022

Introduction

À propos

Quelques bouts de code:

Conversion de flottants en base 10
(`https://pkg.go.dev/strconv`)

Suite de tests pour l'arrondi de flottants:
`github.com/remyoudompheng/fptest`

Implémentation avec Sage de l'attaque de Castryck et Decru
`https://github.com/jack4818/Castryck-Decru-SageMath`

Le papier

"Projective Geometry of Hessian Elliptic Curves and Genus 2 Triple Covers of Cubics"

`https://eprint.iacr.org/2022/1107`

Quelques changements dans cet exposé!

Le code:
`https://github.com/remyoudompheng/elliptic-gluing3`

(200 lignes de Python/Sage et des tests)

Motivation

Implémentation de l'attaque de Castryck et Decru sur SIDH.

Ingrédient principal: isogénies de degré $(2, 2)$ entre surfaces abéliennes.

Comment calquer le calcul en degré $(3, 3)$?

De préférence avec des calculs similaires (correspondances entre courbes, coordonnées de Mumford).

Protagonistes

Courbes elliptiques: $y^2 = x^3 + ax + b$

Courbes de genre 2: $y^2 = F(x)$ (de degré 6)

(et un peu les jacobiennes $\mathrm{Jac}(H) \dashrightarrow \mathrm{Sym}^2(H)$)

Le problème du recollement

Comprendre les isogénies $E_1 \times E_2 \to S$ où S est une surface abélienne ou une jacobienne de courbe de genre 2.

Théorème (Kuhn)

Si H est une courbe de genre 2 et $H \to E$ est un revêtement de degré d «primitif» (sans factorisation non triviale), la jacobienne de H admet une isogénie de degré (d, d) vers un produit $E \times E'$.

Le théorème de Kani

Classification des constructions de recollement.

Utilisé dans la méthode de Castryck et Decru en degré 2^k.

Théorème (Kani)

Les isogénies (primitives) $E_1 \times E_2 \to S$ de degré N sont en bijection avec les revêtements (ramifiés) de degré N de la forme $H \to E_1$ et $H \to E_2$ par une courbe de genre 2. Cette courbe est singulière si et seulement si elle est le graphe de deux correspondances duales de degrés (d_1, d_2) avec $d_1 + d_2 = N$.

Problème reformulé

Étant donné deux courbes elliptiques, trouver H de genre 2 et des morphismes $H \to E_i$ de la forme

$$(x, y) \to \left(\frac{N(x)}{D(x)}, y \cdot \frac{R(x)}{D(x)^2} \right)$$

avec N, R, D de degré 3.

Tout morphisme de degré 3 est de cette forme et le choix de la bijection $E_1[3] \simeq E_2[3]$ doit déterminer une solution canoniquement.

État de l'art sur les isogénies entre surfaces abéliennes

Constructions géométriques: en degré 2, isogénies de Richelot, en degré 3 via les surfaces de Kummer (BLP, Dolgachev-Lehavi).

Pour un produit de courbes elliptiques, morphismes de recollement (BHLS)

Fonctions thêta, surfaces de Kummer pour une surface abélienne quelconque (Robert, Lubicz, Cosset).

Cas du produit de courbes elliptiques

Kuhn donne une forme générale pour H:

$$y^2 = (x^3 + ax^2 + bx + c)(4cx^3 + b^2x^2 + 2bcx + c^2)$$

avec des morphismes:

$$(x, y) \mapsto \left(\frac{x^2}{x^3 + ax^2 + bx + c}, ?? \right)$$

$$(x, y) \mapsto \left(\frac{(x-d)^2(x-e)}{4cx^3 + b^2x^2 + 2bcx + c^2}, ?? \right)$$

Une famille universelle (BHLS)

Formules (Bröker-Howe-Lauter-Stevenhagen)

Une famille paramétrée par $\{12ac + 16bd = 1\}/\mathbb{G}_m$

$$
\begin{aligned}
H : y^2 &= (x^3 + 3ax + 2b)(2dx^3 + 3cx + 1) \\
E_1 : y^2 &= x^3 + 12(2a^2d - bc)x^2 + 12(16ad^2 + 3c^2)(a^3 + b^2)x \\
&\quad + 512(a^3 + b^2)^2 d^3 \\
E_2 : y^2 &= x^3 + 12(2bc^2 - ad)x^2 + 12(16b^2c + 3a^2)(c^3 + d^2)x \\
&\quad + 512(c^3 + d^2)^2 b^3
\end{aligned}
$$

Pour un choix de $j(E_i)$ on doit avoir 24 solutions correspondant aux anti-isométries $E_1[3] \simeq E_2[3]$.

Utilisation en pratique

Un avantage de la famille de BHLS: fonctionne aussi pour une 3-torsion non rationnelle.

Trop de solutions sans fixer la structure de niveau (polynôme de degré > 10).

Comment choisir le paramètre si on a fixé une anti-isométrie? Calculer le noyau de l'isogénie?

Forme de Hesse des courbes elliptiques

Toute courbe elliptique munie d'un choix de base de $E[3]$ est projectivement équivalente à

$$E_t : x^3 + y^3 + z^3 = 3txyz$$

où t appartient à $\mathcal{X}(3) = \mathbb{A}^1 \setminus \mu_3$

Résultat

On peut construire sur la base $\mathcal{X}(3) \times \mathcal{X}(3)$ une famille universelle de courbes génériquement de genre 2 (à réduction stable) munie de projections de degré 3 $H_{t_1,t_2} \to E_{t_i}$.

Pour des paramètres t_1, t_2 choisis, la courbe H_{t_1,t_2} est un revêtement double d'une sextique plane rationnelle (dont les coordonnées des points doubles sont calculables) ramifié en des points correspondant aux points de Weierstrass de E_1 et E_2.

En pratique

Algorithme

- Calculer des coordonnées (x_1, x_2) de points doubles
- Trouver une (unique) sextique plane passant par ces points
- Résoudre les singularités par 2 transformations quadratiques
- Calculer une paramétrisation rationnelle (~~une racine carrée~~)
- Choisir une équation hyperelliptique (~~une racine carrée~~)

Propriétés

- Cas particulier (un point triple, une seule transformation quadratique).
- Cas singulier: en cas de 2-isogénie, courbe stable au lieu de genre 2
- Calcul rapide (pas de racine de polynôme à calculer).

Construction et géométrie

Forme hessienne des courbes elliptiques

Équations de type (avec $t^3 \neq 1$)

$$x^3 + y^3 + z^3 = 3txyz$$

Les points de 3-torsion sont les permutations cycliques de $(1, -j^k, 0)$ où j est une racine cubique de l'unité.

Les translations ont une représentation linéaire:
$[x : y : z] \to [y : z : x]$ et $[x : y : z] \to [x : jy : j^2 z]$ qui ne dépend pas de t! (groupe de Heisenberg)

Bibliographie

- Dolgachev, *Classical Algebraic Geometry*
- Artebani, Dolgachev, *The Hesse pencil of plane cubic curves*

Des points et des droites

On cherche à faire correspondre à un point de E_1 trois points de E_2.

La composée $E_1 \to Jac(H) \to E_2$ doit être nulle donc ces points sont alignés

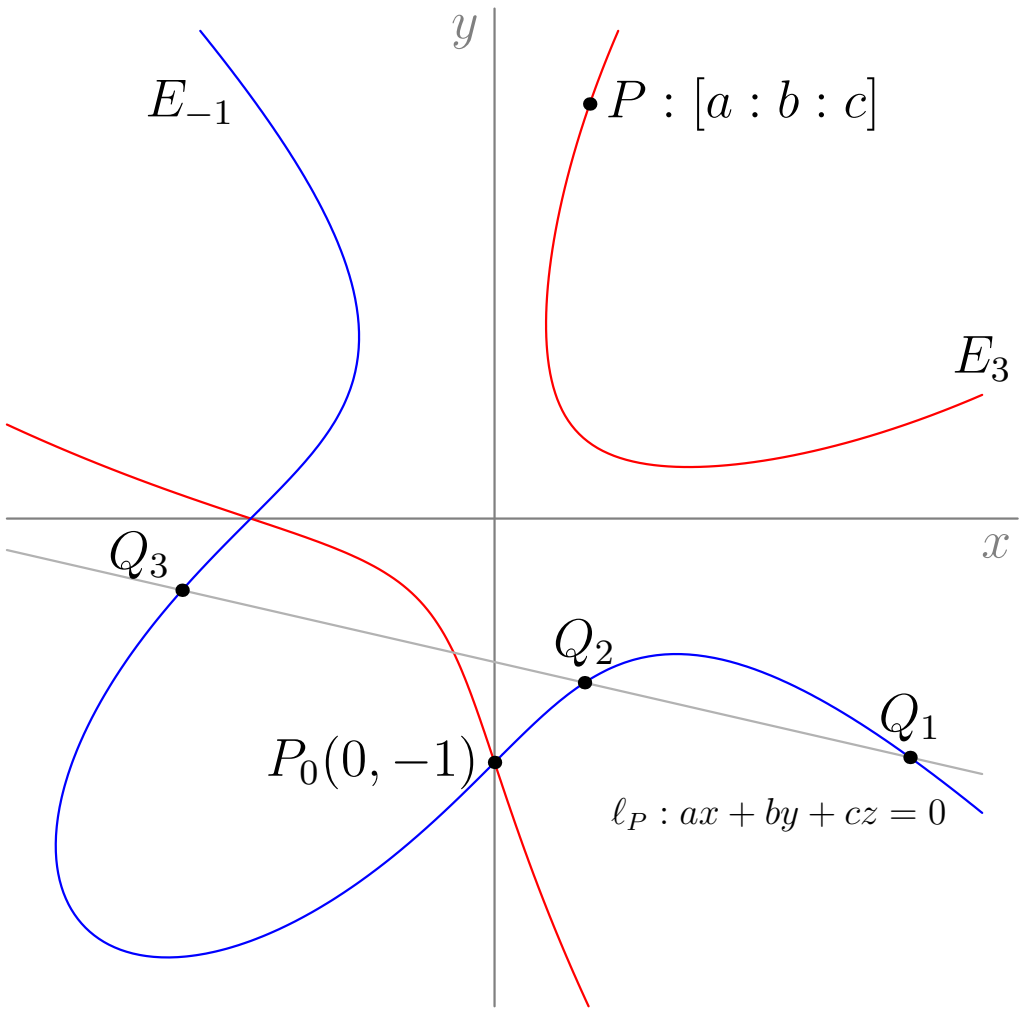
Candidat naturel: une relation de polarité $\mathbb{P}^2 \to (\mathbb{P}^2)^\vee$.

Polarité

Relation d'équation:

$$x_1x_2 + y_1y_2 + z_1z_2 = 0$$

Point $\leftrightarrow$ droite orthogonale
Définit une courbe $\tilde{H}$ dans $E_1 \times E_2$



Quelques observations

Le genre de $\tilde{H}$ peut se calculer par théorie d'intersection ($g = 10$)

Le groupe $\Gamma \subset E_1[3] \times E_2[3]$ agit trivialement sur l'équation de $\tilde{H}$.

Et l'action est sans point fixe: le quotient de $\tilde{H}$ est non ramifié de genre 2.

Lien avec les fonctions thêta

La courbe choisie est un diviseur de $|3\Theta| = |\mathcal{O}(1,1)|$ dans $E_1 \times E_2$ qui est symétrique et invariant par Γ.

Son quotient est un diviseur thêta et une polarisation principale sur $E_1 \times E_2/\Gamma$.

Question

Peut-on calculer ses thêta-constantes? Un point de la quartique de Burkhardt? Via des polynômes modulaires?

Dérivées

La dérivée de l'équation

$$x_1x_2 + y_1y_2 + z_1z_2 = 0$$

au point (P_1, P_2) est:

$$\langle P_1, dP_2\rangle + \langle dP_1, P_2\rangle = 0$$

On peut donc interpréter géometriquement la ramification et les singularités.

Cas singulier et courbe caylayenne

Soit W un point d'ordre 2. Le lieu des droites $\phi(P) = (P, P + W)$ est aussi une courbe Hessienne.

$P \to (P, P + W)$ est une isogénie de noyau W.

La polarité est $\phi(P) \leftrightarrow \{P, P + W, W - 2P\}$.

La correspondance $\phi(P) \mapsto W - 2P$ est le graphe de l'isogénie duale.

La correspondance $\{P, P + W\} \mapsto \phi(P)$ est le graphe de ϕ.

Egalité si $3P = W$.

En géométrie projective classique l'isogénie est entre la courbe hessienne et la courbe cayleyenne.

Projection sur une courbe plane

$$\begin{array}{ccccccc} \tilde{H} & \longrightarrow & H & \longrightarrow & \bar{H} & \longrightarrow & \bar{H}_\iota \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ E_1 \times E_2 & \longrightarrow & (E_1 \times E_2)/\Gamma & \longrightarrow & E_1 \times E_2 & \longrightarrow & \mathbb{P}^1 \times \mathbb{P}^1 \end{array}$$

La courbe $\bar{H}_\iota$ est rationnelle et de degré $(3, 3)$.

La composée $E_1 \times E_2 \to E_1 \times E_2$ est la multiplication par 3.

Singularités et formules

Cartographie

Pour comprendre la structure du revêtement triple on projette sur l'axe des abscisses

$$E_1 \times E_2 \to \mathrm{Jac}(H) = E_1 \times E_2/\Gamma \to E_1 \times E_2 \to \mathbb{P}^1 \times \mathbb{P}^1$$

Théorème

La projection de H sur $E_1 \times E_2$ est une courbe singulière à 8 points doubles (ou 2 point triples et 2 point doubles).
La projection de H sur $\mathbb{P}^1 \times \mathbb{P}^1$ est une courbe rationnelle de degré $(3, 3)$ à 4 points doubles (ou un point triple et un point double).

Le point de ramification

Point de ramification de $H \to E_2$

2 points conjugués par l'involution hyperelliptique (Riemann-Hurwitz)

Intersection entre E1 et la courbe duale de E2

Calcul explicite par élimination

Coordonnées rationnelles en t_1 et t_2:

$$x_1 = \frac{4t_1^2t_2^3 - t_1^2 - t_2^4 - 6t_1t_2^2 + 4t_2}{4(t_1^3 - 1)(t_2^3 - 1)}$$

Une autre polarité

La projection de H sur $E_1 \times E_2$ doit aussi être définie par une relation de polarité!

Théorème

Il existe une relation bilinéaire b telle que $b(3P, 3Q) \iff P \perp Q$

Calcul effectif

La matrice peut se calculer par simulation numérique.

On obtient une matrice de fractions rationnelles en t_1 et t_2.

Son déterminant peut s'annuler (exactement dans la situation des points triples).

$$\det = (t_1^3 - 1)^2 (t_2^3 - 1)^2 (t_1 t_2 - 1)$$
$$(t_1 + t_2 + 1)(t_1 + jt_2 + j^2)(t_1 + j^2 t_2 + j)$$

Correspondance en forme de Weierstrass

Si E_i sont écrites en forme de Weierstrass H peut être décrite par:

$$S(x_1, x_2) = 0$$

$$y_1 y_2 = Q(x_1, x_2)$$

S est l'équation de la courbe rationnelle de degré $(3, 3)$

Q est un changement de coordonnées sur la matrice précédente:

$$Q = t_1 x_1 + t_2 x_2 - x_1 x_2 (t_1 t_2 + 2) - \frac{1}{3} - \frac{2(t_1 t_2 - 1)^3}{3(t_1^3 - 1)(t_2^3 - 1)}$$

Points singuliers de la représentation plane

Correspond à une relation $P \sim Q$ et $P \sim Q + T$ où $3T = 0$.

Equation de $(Q, Q + T)$:

$$(x : y : z) \wedge (x : jy : j^2 z) = (j^2 - j)[yz : jzx : j^2 xy]$$

On retrouve une transformation quadratique du plan, équations très simples.

Pour chaque T on a 18 points de $\tilde{H}$ donc un seul point de $\mathbb{P}^1 \times \mathbb{P}^1$, on s'attend donc à trouver une section rationnelle: l'abscisse doit être une fonction rationnelle de t_1 et t_2.

Formules explicites pour les points doubles

L'abscisse des points doubles a des formules explicites: (pour l'autre coordonnée, échanger t_1 et t_2, j et j^2).

$$u(P_0) = \frac{t_1^2 - t_2}{t_1^3 - 1}$$

$$u(P_1) = \frac{t_1 t_2 - 1}{(t_1 - 1)(t_1 - j^2)(t_2 - j^2)}$$

$$u(P_2) = \frac{t_1 t_2 - 1}{(t_1 - 1)(t_1 - j)(t_2 - j)}$$

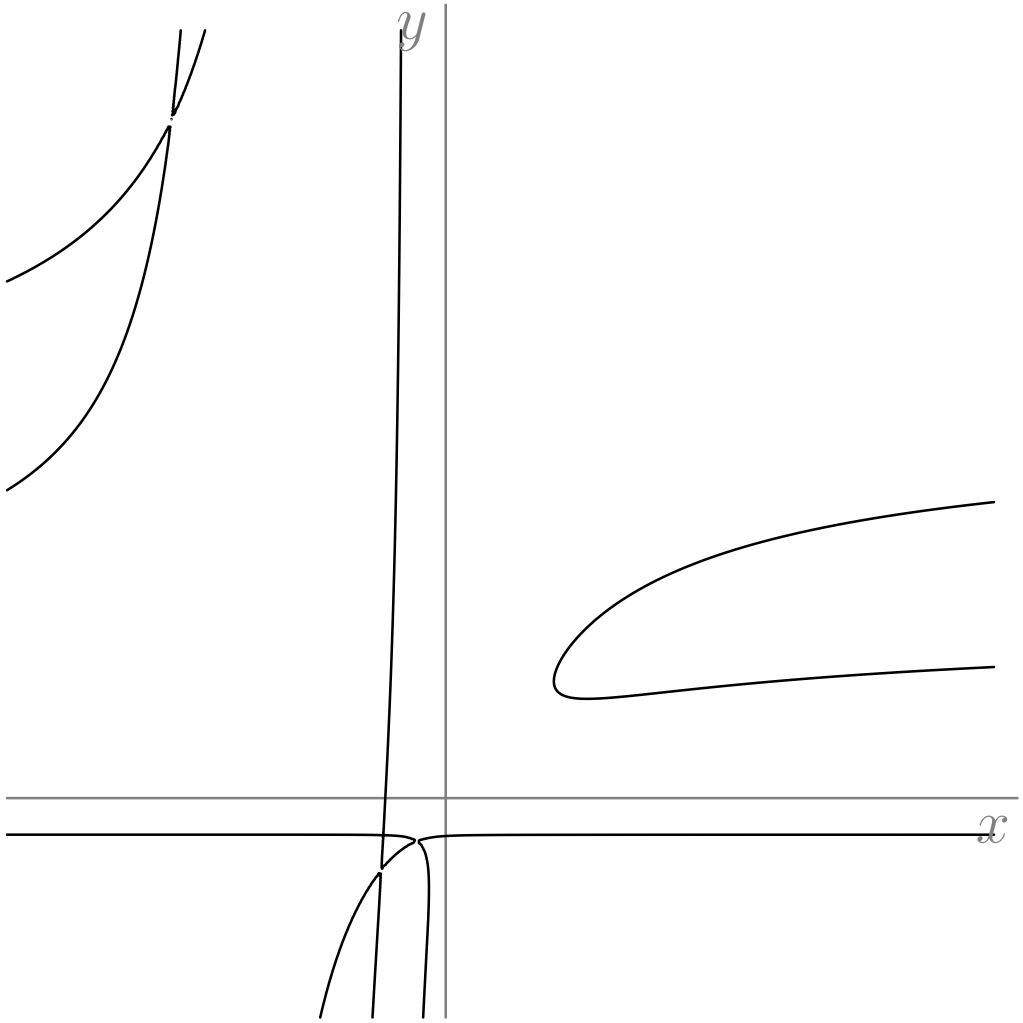
$$u(P_3) = \frac{t_1 t_2 - 1}{(t_2 - 1)(t_1 - j)(t_1 - j^2)}$$

Équation de la sextique

4 points doubles

$$x = \frac{t^3 - t - 1}{(t-4)(t-1)(t+4)}$$

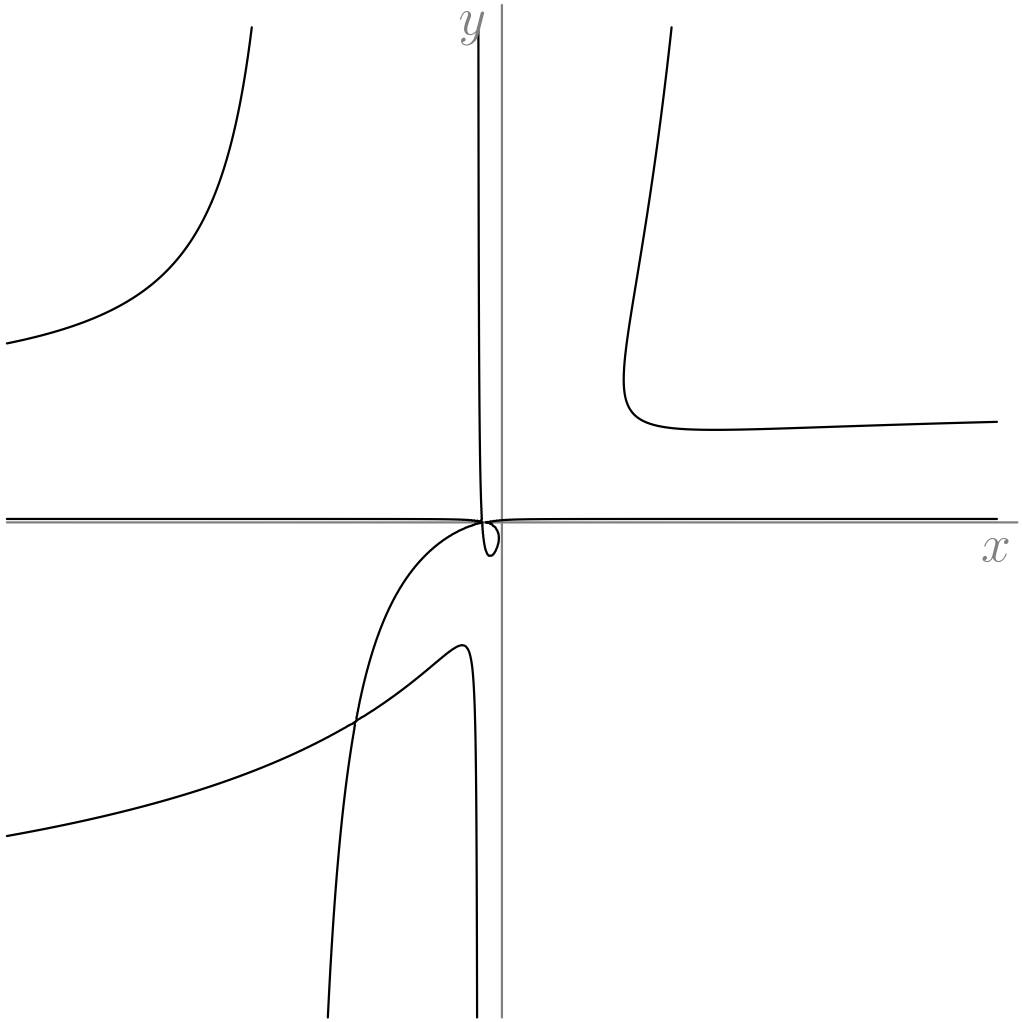
$$y = \frac{t^3 - 3t + 1}{(t+2)(t+5)(t-3)}$$



Point triple

$$x \simeq \frac{t^3 + t - 3}{(t-4)(t-1)(t+4)}$$

$$y \simeq \frac{t^3 - 2t + 9}{(t+2)(t+3)(t-3)}$$



Implémentation et commentaires

Étapes

Déterminer les points doubles

Trouver la sextique (unique!)

Résoudre les points doubles par une ou deux tranformations quadratiques

Déterminer une équation hyperelliptique de H

Équation de la sextique

La sextique doit passer par les points de Weierstrass

$$S(u_1, \infty) = P_1(u_1)$$

$$S(\infty, u_2) = P_2(u_2)$$

On utilise les coordonnées des points multiples

(fractions rationnelles en t_1 et t_2)

On obtient un système linéaire surdéterminé.

Résolution des singularités

Transformation quadratique standard

Si une courbe $f(x, y, z) = 0$ a multiplicité a au point $[1 : 0 : 0]$, b au point $[0 : 1 : 0]$, c au point $[0 : 0 : 1]$, son image par la transformation rationnelle $[x : y : z] \mapsto [yz : zx : xy]$ a pour équation $f(yz, zx, xy)/(x^a y^b z^c)$.

2 points triples, 1 point double: degré $d \mapsto 2d - 8$.

3 points doubles: degré $d \mapsto 2d - 6$.

2 cas:

- sextique $\to$ quartique $\to$ conique
- sextique $\to$ cubique nodale

Pas besoin d'opérations sur les coefficients!

Paramétrage rationnel

On peut trouver un point rationnel sur une conique avec O(1) racines carrées (sur un corps fini).

Mais le point de ramification est rationnel ! (tout polynôme de degré 3 avec une racine double a une racine rationnelle)

Détermination de l'équation

Une fois qu'on a un paramétrage de degré $(3, 3)$:

$$T \mapsto (x_1 = N_1/D_1, x_2 = N_2/D_2)$$

On définit $H : y^2 = \alpha D_1 D_2$

et les morphismes:

$$(x, y) \mapsto (N_1(x)/D_1(x), yR_1(x)/D_1(x)^2)$$

$$(x, y) \mapsto (N_2(x)/D_2(x), yR_2(x)/D_2(x)^2)$$

On exprime R_1 et R_2 en fonction de racines carrées de polynômes unitaires (ok) et d'une racine carrée de $P_1(x_1(\infty))P_2(x_2(\infty))$.

Exemple numérique

Sur $\mathbb{F}_{37}$ équations de Hesse et forme de Weierstrass

$$E_1 : x^3 + y^3 + z^3 = 3 \cdot 22xyz$$
$$E_2 : x^3 + y^3 + z^3 = 3 \cdot 34xyz$$
$$E_1 : v^2 = P_1(u) = 25(u^3 + 10u^2 + 21u + 36)$$
$$E_2 : v^2 = P_2(u) = 34(u^3 + 30u^2 + 36u + 33)$$

La sextique dans $\mathbb{P}^1 \times \mathbb{P}^1$:

$$u_1^3u_2^3 + 10u_1^2u_2^3 + 21u_1u_2^3 + 36u_2^3$$
$$+30u_1^3u_2^2 + 36u_1^3u_2 + 33u_1^3$$
$$+8u_1^2u_2^2 + 7u_1u_2^2 + 4u_1^2u_2 - 9u_1u_2 + 16u_2 - 12u_1 - 8$$

Exemple numérique

Résolution des singularités:

Degré 4:

$$11x^3y - 9x^2y^2 - 4xy^3 - 2x^3z - 16x^2yz + 11xy^2z$$

$$-17y^3z - 10x^2z^2 + 15xyz^2 - y^2z^2 - 9xz^3 + 7yz^3 + z^4$$

Degré 2 (conique):

$$3x^2 + 14xy + y^2 - 6xz - 18yz - 17z^2$$

Exemple numérique

Paramétrage rationnel:

$$\frac{19T^2+5T+13}{T^3+10T^2+4T+21} \quad \frac{26T^3+23T^2+13T+7}{T^3+29T^2+32T+13}$$

$$P_1(u_{1,\infty}) = 12 \quad P_2(u_{2,\infty}) = 1 \quad \sqrt{12} = 7$$

$$\sqrt{P_1(u_1)P_2(u_2)} = t_1u_1+t_2u_2-u_1u_2(t_1t_2+2)-\frac{1}{3}-\frac{2(t_1t_2-1)^3}{3(t_1^3-1)(t_2^3-1)}$$

$$H : y^2 = 12(T^3 + 10T^2 + 4T + 21)(T^3 + 29T^2 + 32T + 13)$$

Morphismes vers E_1 et E_2:

$$(T, y) \mapsto \left(\frac{19T^2 + 5T + 13}{T^3 + 10T^2 + 4T + 21}, y \frac{12T^3 + 17T^2 + 30T + 17}{12(T^3 + 10T^2 + 4T + 21)^2} \right)$$

$$(T, y) \mapsto \left(\frac{26T^3 + 23T^2 + 13T + 7}{T^3 + 29T^2 + 32T + 13}, y \frac{T^3 + 10T^2 + 2T + 5}{7(T^3 + 29T^2 + 32T + 13)^2} \right)$$

Performance et complexité

Coût asymptotique: ~~2 racines carrées~~

Quelques centaines d'opérations élémentaires du corps de base.